

Docket No.: 324-160

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of :
Sylvie CAMUS et al. :
U.S. Patent Application No. : Group Art Unit:
Filed: Herewith : Examiner:

For: DELEGATION BY ELECTRONIC CERTIFICATE

CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

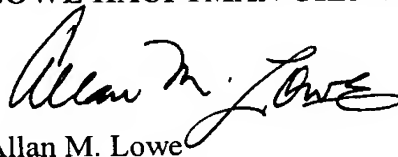
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicant hereby claims, in the present application, the priority of France Patent Application No. 02-13179, filed October 22, 2002. The certified copy is submitted herewith.

Respectfully submitted,

LOWE HAUPTMAN GILMAN & BERNER, LLP



Allan M. Lowe
Registration No. 19,641

1700 Diagonal Road, Suite 310
Alexandria, Virginia 22314
(703) 684-1111 AML/ssw
Facsimile: (703) 518-5499
Date: October 15, 2003



BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 15 SEP. 2009

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr



26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa
N° 11354*03

REQUÊTE EN DÉLIVRANCE

page 1/2

BR1

Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 0 W / 210502

REMISE DES PIÈCES DATE 22 OCT. 2002 LIEU 99 N° D'ENREGISTREMENT 0213179 NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE 22 OCT. 2002 PAR L'INPI		1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE ■ CABINET MARTINET & LAPOUX Conseils en Propriété Industrielle 43 boulevard Vauban B.P. 405 GUYANCOURT 78055 ST QUENTIN YVELINES CEDEX ■	
Vos références pour ce dossier SD/CNET04396 <i>(facultatif)</i>			
Confirmation d'un dépôt par télécopie <input type="checkbox"/> N° attribué par l'INPI à la télécopie		2 NATURE DE LA DEMANDE Cochez l'une des 4 cases suivantes	
Demande de brevet <input checked="" type="checkbox"/>		<input type="checkbox"/>	
Demande de certificat d'utilité <input type="checkbox"/>		<input type="checkbox"/>	
Demande divisionnaire <input type="checkbox"/>		<input type="checkbox"/>	
Demande de brevet initiale ou demande de certificat d'utilité initiale		N° <input type="text"/> Date <input type="text"/> N° <input type="text"/> Date <input type="text"/>	
Transformation d'une demande de brevet européen <i>Demande de brevet initiale</i>		<input type="checkbox"/> N° <input type="text"/> Date <input type="text"/>	
3 TITRE DE L'INVENTION (200 caractères ou espaces maximum) Délégation par certificat électronique			
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation <input type="text"/> N° <input type="text"/> Date <input type="text"/> Pays ou organisation <input type="text"/> N° <input type="text"/> Date <input type="text"/> Pays ou organisation <input type="text"/> N° <input type="text"/> Date <input type="text"/> <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
5 DEMANDEUR (Cochez l'une des 2 cases)		<input checked="" type="checkbox"/> Personne morale <input type="checkbox"/> Personne physique	
Nom ou dénomination sociale		FRANCE TELECOM	
Prénoms		Société Anonyme	
Forme juridique		13 8 0 1 2 9 8 6 6	
N° SIREN		1 1 1 1	
Code APE-NAF		6, Place d'Alleray	
Domicile ou siège	Rue	17 5 0 1 1 5 PARIS	
	Code postal et ville	FRANCE	
	Pays	Française	
Nationalité		N° de télécopie <i>(facultatif)</i>	
N° de téléphone <i>(facultatif)</i>		<input type="checkbox"/> S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»	
Adresse électronique <i>(facultatif)</i>		Remplir impérativement la 2 ^{ème} page	



1er dépôt

**BREVET D'INVENTION
CERTIFICAT D'UTILITÉ****REQUÊTE EN DÉLIVRANCE**
page 2/2**BR2**

REMISE DES PIÈCES DATE 22 OCT. 2002 LIEU 99 N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0213179		Réservé à l'INPI	
6 MANDATAIRE (s'il y a lieu)			
Nom		LAPOUX	
Prénom		Roland	
Cabinet ou Société		CABINET MARTINET & LAPOUX	
N° de pouvoir permanent et/ou de lien contractuel			
Adresse	Rue	43 boulevard Vauban B.P. 405 GUYANCOURT	
	Code postal et ville	17180 51 ST QUENTIN YVELINES CEDEX	
	Pays	FRANCE	
N° de téléphone (facultatif)		01 30 64 90 09	
N° de télécopie (facultatif)		01 30 64 90 02	
Adresse électronique (facultatif)		martinet@wanadoo.fr	
7 INVENTEUR (S)		Les inventeurs sont nécessairement des personnes physiques	
Les demandeurs et les inventeurs sont les mêmes personnes		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non : Dans ce cas remplir le formulaire de Désignation d'inventeur(s)	
8 RAPPORT DE RECHERCHE		Uniquement pour une demande de brevet (y compris division et transformation)	
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> <input type="checkbox"/>	
Paiement échelonné de la redevance (en deux versements)		Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt <input type="checkbox"/> Oui <input type="checkbox"/> Non	
9 RÉDUCTION DU TAUX DES REDEVANCES		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Obtenue antérieurement à ce dépôt pour cette invention (joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence) : AG [] [] [] [] [] []	
10 SÉQUENCES DE NUCLEOTIDES ET/OU D'ACIDES AMINÉS		<input type="checkbox"/> Cochez la case si la description contient une liste de séquences	
Le support électronique de données est joint		<input type="checkbox"/>	
La déclaration de conformité de la liste de séquences sur support papier avec le support électronique de données est jointe		<input type="checkbox"/>	
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes			
11 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)		VISA DE LA PRÉFECTURE OU DE L'INPI	
Roland LAPOUX Mandataire CPI/92-1136		L. GUICHET	

Délégation par certificat électronique

La présente invention concerne la délégation de moyens cryptographiques par certificat électronique.

5

Etant donnée une clé cryptographique composée d'une clé publique et d'une clé privée, l'objet fondamental permettant d'avoir confiance en la clé publique est un certificat électronique émis par une autorité de certification. Ce certificat comprend
10 notamment la clé publique à certifier, l'identité du possesseur de la clé publique, une période de validité de certificat, une liste d'attributs d'utilisation de clé correspondant à des droits d'utilisation de la clé appelés "key usages",
15 supportant des paramètres tels que par exemple une clé de signature de message ou une clé de serveur web sécurisé, et une signature cryptographique des données ci-dessus contenues dans le certificat par une clé publique de l'autorité de certification
20 émettrice du certificat.

La confiance en la clé publique associée à une identité se ramène à la validité du certificat qui dépend notamment de la validité d'une "chaîne de confiance" du certificat C. La "chaîne de confiance"
25 du certificat C est une suite finie de N certificats $C_1, C_2, \dots, C_n, C_{n+1}, \dots, C_N$ émis par des autorités de certification respectives $AC_2, AC_n, \dots, AC_{n+1}, \dots, AC_N$, le premier certificat C_1 étant le certificat à vérifier C. La suite finie de la "chaîne de confiance" se termine par un certificat C_N explicitement déclaré "certificat de confiance". Un
30 certificat C_n est certifié par l'autorité de certification AC_{n+1} qui émet un certificat C_{n+1} . En général, le certificat de confiance C_N est une racine
35

de la chaîne de confiance et constitue un certificat auto-signé par une autorité de certification bien connue de la communauté des autres autorités de certification amenées à s'y référer. Une chaîne de confiance est validée par la validité individuelle de chacun des certificats C_n ainsi que par la validité du chaînage au niveau de chaque autorité de certification AC_{n+1} de manière à assurer que l'autorité de certification AC_{n+1} a bien signé le certificat C_n en le certificat C_{n+1} .

Les attributs d'utilisation de clé d'une autorité de certification inclus dans le certificat émis par cette autorité spécifient notamment la profondeur de certification autorisée. Une autorité de certification ne pouvant certifier que des usagers finaux ou des serveurs a une profondeur de certification autorisée minimale, par exemple égale à zéro. Un usager final a un attribut mentionnant qu'il n'a pas le droit d'émettre des certificats. Lorsque cet attribut n'est pas mentionné, on suppose par défaut que l'utilisateur n'a pas le droit d'émettre des certificats ; par convention, la profondeur de certification autorisée du certificat vaut -1.

Une signature électronique garantit l'authenticité d'un document, c'est-à-dire authentifie de façon sûre un ou des signataires ayant exécuté la signature, et garantit que le document n'a pas été modifié. La signature électronique est souvent utilisée pour garantir la non-répudiation du document qui consiste à se prémunir contre un déni de l'auteur du document.

Selon une autre technique dite "multi-acteurs" ("multi-agents"), la signature électronique est une signature de groupe qui assure l'anonymat au

signataire appartenant au groupe, en signant au nom du groupe.

Les formats connus de signature électronique n'offrent pas de moyen d'inclure une mention de
5 délégation de signature.

Peu de systèmes de signature électronique permettent actuellement une délégation de signature. En particulier, aucun de ces systèmes ne prévoit une
10 délégation de clés cryptographiques certifiées.

Lorsqu'une délégation de signature existe dans un système de signature électronique, elle concerne en général une délégation de droits, avec un moyen de gestion d'habilitations effectuée en interne par le
15 système, ou dans les meilleurs cas via un annuaire plus général.

Par exemple, dans un flux de travail ("workflow") peut être défini un groupe de "titulaires" qui ont le droit de prendre des
20 décisions au sein du système. Pour pallier les absences des titulaires, un ou plusieurs "délégués" peuvent être adjoints à chacun des titulaires.

Sur décision d'un titulaire, par exemple lors d'une action dans le flux de travail comme une
25 déclaration de congés, tout ou partie des habilitations du titulaire sont attribuées au délégué pendant une période de délégation prédéterminée afin de ne pas induire une rupture de fonctionnement dans le flux de travail. Les décisions prises par le
30 délégué au sein du flux de travail le seront au nom du titulaire.

Le plus souvent, la trace de la délégation est perdue une fois la période de délégation achevée. Dans les meilleurs cas, la délégation est retrouvée
35 en dépouillant des relevés ou registres (logs) du

flux de travail, moyennant une opération de recherche complexe et coûteuse, surtout si la recherche doit être effectuée longtemps après.

5 Dans le cas de flux de travail incluant de la signature électronique, où l'objet de la "décision" est la signature électronique d'un document, il n'est pas prévu dans les formats de signature électronique existants un champ "signé au nom de" permettant de retrouver le titulaire au nom duquel la signature a
10 été effectuée par le délégué. Le document signé, une fois sorti du cadre du flux de travail pour être traité par un tiers ou archivé, par exemple, ne comporte plus que la signature du délégué, sans trace du titulaire au nom duquel le délégué a effectué la
15 signature.

La délégation de pouvoir n'étant pas incluse dans la signature électronique ne peut donc pas être retrouvée une fois que le document signé est sorti de son contexte de délégation.

20 Or, la signature électronique doit être persistante, et avec elle doivent persister les éléments pour retrouver les conditions sous lesquelles la signature a été exécutée, comme par exemple l'adjonction de la mention écrite "par
25 intérim" dans le cas d'une signature manuscrite.

En outre, la délégation nécessite souvent, soit pour le titulaire, soit pour le délégué, soit pour les deux, une intervention auprès du moyen de gestion habilitant les délégations.

30 La présente invention a pour objectif principal de permettre au délégué d'effectuer des actions cryptographiques avec sa clé sous l'autorité directe du titulaire, sans recourir par ailleurs à une
35 autorité de certification, et d'introduire une trace

de la délégation dans le certificat utilisé par le délégué au nom du titulaire.

5 Pour atteindre cet objectif, un procédé de certification électronique pour déléguer des actions d'un titulaire ayant un certificat électronique mémorisé dans un terminal de titulaire à un délégué ayant un premier certificat électronique mémorisé dans un terminal de délégué, le certificat du
10 titulaire et le premier certificat du délégué comportant en outre des clés publiques respectives et des signatures de certificat d'autorités de certification respectives, est caractérisé en ce que, après une sollicitation de délégation du délégué par
15 le titulaire, il comprend les étapes suivantes :

- dans le terminal de délégué, un établissement d'une requête de re-certification et une transmission de la requête de certification au terminal de titulaire,
- 20 - un établissement d'un deuxième certificat de délégué électronique dans le terminal de titulaire en réponse à la requête de re-certification, et une transmission du deuxième certificat au terminal de délégué, le deuxième certificat incluant des données
25 telles que la clé publique du titulaire, la clé publique de délégué et un attribut de délégation, et une signature des données avec une clé privée du titulaire,

- dans le terminal de délégué, une validation de
30 la signature dans le deuxième certificat de délégué transmis afin que le terminal utilise le deuxième certificat validé pour toute action déléguée par le titulaire au délégué.

35 L'invention hisse ainsi le titulaire en une autorité de certification pour le délégué, puisque

les données contenues dans le deuxième certificat et particulièrement la clé publique de délégué sont signées par le titulaire.

5 La trace de la délégation est représentée par l'attribut de délégation. De préférence, cette trace est complétée ou remplacée par un attribut représentant une autorisation du titulaire à déléguer inclus dans le certificat du titulaire qui lui-même peut être inclus dans les données du deuxième
10 certificat du délégué.

D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture de la description suivante de plusieurs
15 réalisations préférées de l'invention en référence aux dessins annexés correspondants dans lesquels :

- la figure 1 est un bloc-diagramme schématique d'un système de télécommunications avec un terminal de titulaire et un terminal de délégué et divers
20 serveurs pour la mise en oeuvre du procédé de certification électronique selon l'invention; et

- la figure 2 est un algorithme d'étapes principales du procédé de certification électronique de l'invention.

25

En référence à la figure 1, deux terminaux TET et TED sont respectivement attribués à un usager titulaire T et un usager délégué D. Les deux terminaux sont reliés par un réseau de
30 télécommunications RT. Par exemple, les terminaux TET et TED sont des ordinateurs personnels et le réseau RT est un réseau local LAN du type Ethernet ou sans fil WAN, ou comprend des réseaux d'accès reliés par le réseau internet. L'un au moins des terminaux TET
35 et TED peut être un objet électronique portable tel

qu'un assistant numérique personnel PDA ou un ordinateur portable. Selon un autre exemple, au moins l'un des terminaux TET et TED est un radiotéléphone et le réseau RT comprend en outre le réseau de radiotéléphonie cellulaire numérique dont dépend le radiotéléphone.

Initialement, chaque terminal TET, TED a mémorisé un certificat électronique CT, C1D identifiant l'utilisateur respectif T, D et contenant notamment une clé publique KPUBT, KPUBD de l'utilisateur T, D possesseur du certificat, l'identité IDT, IDD comprenant par exemple les nom et prénom de l'utilisateur, une période de validité, éventuellement des attributs ATT, ATD tels que l'identité de l'autorité de certification électronique ACT, ACD ayant créé le certificat, la clé publique de cette autorité et la désignation de l'algorithme servant à signer le certificat, etc. Le certificat CT, C1D comprend également une signature cryptographique SACT, SACD de toutes les données précédentes contenues dans le certificat CT, C1D, établie par l'autorité de certification ACT, ACD ayant émis le certificat. Comme montré à la figure 1, les autorités de certification ACT et ACD sont des serveurs reliées au réseau RT qui ont pour rôle de signer les certificats, de publier les certificats dans des annuaires et d'établir des listes de certificats révoqués, dites listes noires.

Chaque terminal TET, TED contient également une clé privée KPRT, KPRD correspondant à la clé publique KPUBT, KPUBD pour signer des messages à transmettre au moyen d'un algorithme asymétrique prédéterminé AA.

Initialement, il est supposé que le titulaire T est habilité à déléguer des actions au délégué D par

l'autorité de certification ACT. Le titulaire T connaît le délégué D et par conséquent, le terminal TET du titulaire T a déjà mémorisé le premier certificat ClD du délégué D.

5 Une autorisation du titulaire T à déléguer peut être représentée par un attribut d'utilisation de clé (key usage) ATT délivré par l'autorité de certification ACT avec une profondeur de certification autorisée égale à 0 et inclus dans le
10 certificat de titulaire CT ; l'autorité ACT émet alors une politique de certification compatible avec ce type d'attribut d'utilisation de clé. Le titulaire T devient avantageusement une autorité de certification à part entière à des fins de
15 délégation. Le certificat de délégation que le terminal de titulaire TET établit, comme on le verra dans la suite, ne nécessite pas un contrôle plus spécifique que les contrôles dans les autres autorités de certification lors de la validation
20 d'une chaîne de confiance.

 En variante, l'autorité de certification de titulaire ACT représente le droit du titulaire à déléguer à la fois par un attribut d'utilisation de clé (key usage) de l'autorité de certification ACT
25 avec une profondeur de certification autorisée de 0 et par un attribut de délégation spécifique.

 Une certification électronique pour déléguer les actions du titulaire T au délégué D comprend selon
30 l'invention principalement des étapes E1 à E7, comme montré à la figure 2.

 A l'étape E1, l'utilisateur T effectue une sollicitation de délégation SLD du délégué D soit directement lors d'une rencontre des usagers T et D,
35 soit par l'intermédiaire d'un message transmis par le

terminal TET au terminal TED sous la forme par exemple d'un courrier électronique (e-mail).

Selon une autre variante, dans le terminal TED est implémenté un serveur logiciel SRD, par exemple un serveur web HTTP (HyperText Transfer Protocol). Le serveur SRD est un programme s'exécutant dans le terminal TED en réponse à un message de sollicitation de délégation SLD transmis par le terminal TET. Le serveur SRD établit alors une requête de recertification RRC comme décrit ci-après afin de la transmettre au terminal TET. En variante, le serveur SRD est un serveur "client" de courrier électronique qui filtre des messages électroniques de sollicitation SLD en provenance de titulaires autorisés.

Précédemment à l'étape de sollicitation de délégation, quel que soit le type de serveur SRD, celui-ci peut décider d'authentifier le terminal TET soit par signature du message de sollicitation SLD sous forme de courrier électronique, soit par authentification selon un protocole de sécurisation prédéterminé du type SSL (Secure Sockets Layer) pour un serveur du type HTTP, soit par authentification à l'aide d'un identificateur et d'un mot de passe, etc. En pratique, un serveur SRT implémenté dans le terminal TET demande de préférence une authentification d'un serveur SRD, c'est-à-dire une authentification du délégué D par le titulaire T, ou éventuellement une authentification mutuelle entre les serveurs SRD et SRT. Le serveur logiciel SRT est du même type, par exemple HTTP/SSL, que le serveur SRD.

Si le titulaire T sollicitant la délégation n'est pas autorisé à déléguer au délégué D, ou si le

délégué refuse la délégation sollicitée, la sollicitation SLD est rejetée par exemple en transmettant un message de refus prédéterminé depuis le terminal TED vers le terminal TET.

5 A l'étape E2, le terminal TED établit une requête de re-certification RRC. Pour établir celle-ci, l'étape E2 comprend notamment des sous-étapes E21, E22 et E23.

10 A la sous-étape E21, le terminal TED est mis en communication avec un serveur web d'applet SA1 installé par l'autorité de certification ACT du titulaire pour récupérer une applet Java AP1 qui permet au navigateur dans le terminal TED d'établir la requête RRC. Le chargement de l'applet AP1 dans le
15 terminal TED peut être effectué avant l'étape E1 dans la mesure où le terminal TED a déjà établi récemment une requête de re-certification. L'applet AP1 contient notamment un algorithme asymétrique AA1 auquel est appliqué la clé publique KPUBD, en tant
20 que données, et la clé privée KPRD afin de produire une signature électronique SKD de la clé publique du délégué D, à l'étape E22. Puis le terminal TED établit la requête de re-certification RRC en y introduisant la clé publique KPUBD, la signature SKD
25 de celle-ci établie précédemment, et éventuellement le premier certificat C1D permettant au titulaire T de vérifier la confiance dans le délégué D, à la sous-étape E23. La requête établie RRC est transmise par le terminal TED au terminal TET via le réseau RT,
30 à l'étape E3.

 Selon une variante, la requête de re-certification RRC est adressée à l'étape E3 par le terminal TED sous la forme d'un message de courrier électronique (e-mail) au terminal TET.

Après la transmission E3 de la requête de re-certification RRC depuis le terminal TED vers le terminal TET à travers le réseau de télécommunications RT, le terminal TET sauvegarde la requête RRC, par exemple dans le disque dur ou une mémoire RAM de celui-ci, à une sous-étape E41 d'une étape de validation de signature E4 comprenant des sous-étapes E42 à E46.

A la sous-étape E42, le terminal TET communique avec un deuxième serveur d'applet SA2 pour récupérer une applet Java AP2 destinée à vérifier la validité de la requête de re-certification reçue RRC, à moins que l'applet AP2 ait été déjà installée une fois pour toutes dans le terminal TET. Le serveur d'applet SA2 est également sous le contrôle de l'autorité de certification ACT et peut être confondu avec le premier serveur d'applet SA1.

Puis aux sous-étapes E43 à E45, au moyen de l'applet chargée AP2, le terminal de titulaire TET vérifie le format de la requête de re-certification reçue RRC et valide celle-ci par rapport à la signature SKD. La validation de la requête RRC, c'est-à-dire de la signature SKD, est effectuée en appliquant la signature SKD, en tant que données, à l'algorithme AA1 contenu dans l'applet AP2 et la clé publique KPUBD extrait de la requête reçue RRC afin de produire normalement une clé publique KPUBD' qui est comparée à la clé publique KPUBD extraite de la requête RRC, à la sous-étape E46. Si la vérification E43 ou la validation E44-E45 est erronée, le titulaire T peut décider d'arrêter la délégation en cours ou solliciter à nouveau une délégation en émettant une sollicitation de délégation SLD à l'étape E1.

Si la requête RRC est validée, c'est-à-dire en l'occurrence si la clé publique KPUBD est validée à la sous-étape E45, le terminal T affiche la requête de re-certification RRC à la sous-étape E46. Par
5 exemple, le terminal T affiche notamment le certificat C1D qui est extrait de la requête RRC lorsque la requête le contient ou qui est lu dans la mémoire du terminal TET, afin que le titulaire T confirme la validation de la requête reçue RRC et la
10 poursuite de la certification électronique pour délégation en passant à l'étape principale d'établissement de deuxième certificat de délégué E5. En variante, le titulaire n'intervient pas à l'étape E46, et la validation de la requête RRC est
15 entièrement automatique dans le terminal TET.

A l'étape E5, le terminal de titulaire TET établit sur la base du premier certificat C1D un certificat de délégation électronique C2D qui sera à
20 substituer au premier certificat C1D par le terminal de délégué D lorsque le délégué D agira au nom et pour le compte du titulaire T.

Le deuxième certificat de délégué C2D est établi au moyen de la deuxième applet AP2 et contient
25 notamment une clé publique KPUBT du titulaire, la clé publique KPUBD du délégué D, l'identité IDD, un attribut de délégation ATD du type "délégué", ou bien une mention "par procuration de" ou "par intérim de" de préférence suivie du nom du titulaire T, une durée
30 de délégation DD fixée par le titulaire T, et d'autres attributs pouvant être nécessaires pour pouvoir mandater le délégué D. Toutes les données précédentes contenues dans le certificat C2D sont appliquées à un algorithme asymétrique AA2 qui est
35 inclus dans l'applet chargée AP2 et dont la clé est

constituée par la clé privée KPRT du titulaire T correspondant à la clé publique KPUBT. L'algorithme AA2 exécuté à la sous-étape E5 délivre une signature ST du deuxième certificat C2D.

5 Le titulaire T se comporte ainsi comme une autorité de certification électronique pour le délégué D pendant la durée de délégation DD. Le certificat C2D est établi au moyen d'un formulaire affiché à l'écran du terminal TET afin que l'utilisateur T
10 y introduise certaines données telles que la durée de délégation DD, une identité du titulaire telle que le nom ou un surnom du titulaire dans l'attribut de délégation ATD, etc.

 En variante simple, le deuxième certificat C2D
15 ne contient aucune option particulière concernant les attributs, et notamment ne contient pas l'attribut de délégation ATD dans la mesure où le titulaire T ayant émis ce certificat est déjà possesseur d'un certificat l'autorisant à déléguer.

20 Selon une autre variante, un générateur aléatoire dans le terminal de délégué TED génère une deuxième clé publique KPUB2D ainsi qu'une deuxième clé privée KPR2D qui sont dédiées à la délégation et ainsi serviront à sécuriser et échanger des messages
25 avec le terminal TED seulement pour des actions déléguées au délégué D par le titulaire T. Comme indiqué en trait pointillé à l'étape E23 dans la figure 2, la deuxième clé publique KPUB2D est incluse dans la requête de re-certification RRC à l'étape E3,
30 et le terminal de titulaire TET extrait de la requête de certification sauvegardée la clé publique KPUB2D afin de l'introduire dans le deuxième certificat à établir C2D, à la place de la clé publique normale KPUBD du délégué D.



Puis à l'étape E6, l'applet AP2 dans le terminal TET transmet le deuxième certificat C2D au terminal de délégué TED à travers le serveur SRT, le réseau RT et le serveur SRT, ou bien sous la forme d'un message
5 de courrier électronique.

Dans le terminal de délégué TED, l'étape E7 pour valider le deuxième certificat électronique C2D comprend des sous-étapes E71 à E76.

10 A la sous-étape E71, le terminal TED sauvegarde le certificat reçu C2D dans son disque dur ou dans une mémoire RAM par exemple. Puis à la sous-étape E72, le terminal TED récupère dans un troisième serveur d'applet SA3 qui dépend de l'autorité de
15 certification ACT, une troisième applet AP3 destinée à valider le certificat reçu C2D, si l'applet n'est pas déjà chargée dans le terminal TED. Le serveur SA3 peut être confondu avec au moins le serveur SA1 afin de charger une applet AP1 confondue avec l'applet AP3
20 à l'étape E21. Selon une autre variante, les serveurs d'applet SA1, SA2 et SA3 sont fusionnés en un unique serveur qui contient les applets AP1, AP2 et AP3.

Après une vérification du format du certificat reçu C2D à la sous-étape E73, le terminal TED procède
25 à la validation du certificat C2D en appliquant les données contenues dans celui-ci et la clé publique KPubT également incluse dans l'applet AP2 à l'algorithme asymétrique AA2 identifié dans le certificat C2D et récupéré dans l'applet AP3.
30 L'exécution de l'algorithme A2 produit une signature ST' qui est comparée à la signature ST extraite du certificat reçu C2D, à la sous-étape E75. Si aux sous-étapes E73 ou E75, la vérification ou la validation n'est pas satisfaisante, le terminal du
35 délégué TED refuse le deuxième certificat C2D par

exemple en transmettant un message de refus prédéterminé au terminal TET. Dans le cas contraire, le terminal TED mémorise le certificat C2D ainsi validé pendant toute la durée de la délégation DD
5 afin d'utiliser le deuxième certificat C2D et notamment sa clé privée KPRD ou KPR2D pour diverses actions cryptographiques effectuées par le délégué D notamment depuis le terminal délégué TED au nom et pour le compte du titulaire T.

10 Selon le support de la clé composite de délégué [KPUBD, KPRD], le deuxième certificat C2D est intégré plus ou moins automatiquement dans le terminal de délégué TED. Si la clé composite de délégué est une clé logicielle gérée par un navigateur, ou par un
15 outil de récupération et de transfert de message électronique, ou par un système d'exploitation, ou par un serveur logiciel tel que le serveur précité SRD, ou par tout autre logiciel adéquat implémenté dans le terminal TED, le certificat C2D est intégré
20 par ce logiciel dans le terminal TED afin de disposer de ce deuxième certificat en correspondance avec la clé composite de délégué existante pour l'utiliser ultérieurement, pour toutes les actions déléguées.

Selon une autre variante, si la clé composite de
25 délégué [KPUBD, KPRD] ou plus généralement le certificat de délégué C1D est mémorisé dans un support d'enregistrement matériel amovible du terminal de délégué TED, tel qu'une carte à puce ou un jeton USB (token USB (Universal Serial Bus)),
30 l'outil de gestion dans ce support demande lui-même la re-certification de la clé de délégué publique existante et commande l'enregistrement du deuxième certificat de délégué C2D dans le support amovible à l'étape E7. Si une deuxième clé [KPUB2D, KPR2D] est
35 générée à l'étape E2, l'outil de gestion du support



intègre le deuxième certificat C2D. L'introduction du deuxième certificat reçu C2D dans le support matériel amovible est de préférence automatisée, sans l'intervention de l'utilisateur délégué D. Cependant, en
5 variante, cette introduction de deuxième certificat peut être effectuée semi-automatiquement, en invitant par affichage dans le terminal TED le délégué D à insérer le support matériel amovible dans le terminal TED afin d'y mémoriser le certificat C2D. Le support
10 d'enregistrement amovible permet au délégué d'utiliser tout autre terminal pour des actions déléguées, doté d'un lecteur approprié du support d'enregistrement amovible.

Lorsque la clé privée KPRD du délégué D a été
15 compromise, c'est-à-dire est connue par au moins un tiers ou a été subtilisée, le délégué D révoque tous ces certificats reposant sur cette clé, y compris le certificat de délégation C2D. Pour révoquer le certificat C2D, le terminal TED s'adresse à un
20 serveur de révocation qui est connu du délégué D et qui peut être installé par le titulaire et lié au serveur ACD de l'autorité de certification du délégué, ou bien s'adresse directement, ou via un serveur personnel dédié à la révocation de
25 délégation, au serveur d'autorité de certification ACT du titulaire T.

Selon encore une autre variante, lors de l'établissement du certificat de délégation C2D à l'étape E5, le terminal TE inclut dans les données du
30 deuxième certificat C2D des informations relatives à une révocation du certificat C2D, par exemple l'adresse d'un serveur de révocation prédéterminé.

Afin de faciliter l'établissement de la chaîne
35 de confiance depuis le certificat de délégation C2D,

le terminal de délégué TED adjoint le certificat de titulaire CT au certificat de délégation C2D pour toute action déléguée par le titulaire T. Selon cette variante, le certificat CT du titulaire T est également inclus dans les données du deuxième certificat C2D transmis par le terminal de titulaire TET au terminal de délégué TED à l'étape E6 afin que le terminal TED extrait le certificat de titulaire CT du certificat sauvegardé C2D.

10 A partir du certificat de titulaire CT, la chaîne de confiance est établie et vérifiée comme en l'absence de délégation, pour n'importe quelle chaîne de confiance. La vérification de la chaîne de confiance de délégation, c'est-à-dire y compris avec le certificat de délégation C2D, implique la vérification des attributs notamment dans le certificat de titulaire CT par l'autorité de certification ACT et dans le certificat de délégation C2D par le terminal TET.

20

 Selon encore une autre variante, notamment les étapes initiales E2, E3 et E4 relatives à l'établissement et la transmission de la requête de recertification RRC et à la validation de la signature électronique SKD sont supprimées afin d'accroître la rapidité d'exécution de la certification électronique selon l'invention. Dans cette variante, la certification électronique commence avant l'étape d'établissement de certificat E5, par une génération d'une clé privée KPRT du titulaire T dans le terminal TET afin que le terminal TET établisse à l'étape E5 la signature ST des données du certificat C2D avec la clé privée générée KPRT. Les données telles que la clé publique du titulaire KPUBT et celles KPUBD, ATD, DD contenues

25
30
35

dans le premier certificat de délégué C1D ont été
préalablement mémorisées dans le terminal TET. Puis
la clé privée générée KPRT est transmise sensiblement
en parallèle avec le deuxième certificat de délégué
5 électronique C2D au terminal de délégué TED, à
l'étape E6 ; par exemple, la clé privée KPRT est
cryptée dans le terminal TET en fonction d'un mot de
passe composé par le titulaire T, ou transmise par un
canal, tel qu'une transmission orale par téléphone
10 entre le titulaire T et le délégué D, autre que le
canal de transmission entre les terminaux TET et TED
via le réseau RT.

REVENDICATIONS

- 1 - Procédé de certification électronique pour déléguer des actions d'un titulaire (T) ayant un
5 certificat électronique (CT) mémorisé dans un terminal de titulaire (TET) à un délégué (D) ayant un premier certificat électronique (C1D) mémorisé dans un terminal de délégué (TED), le certificat (CT) du titulaire et le premier certificat (C1D) du délégué
10 comportant en outre des clés publiques respectives (KPUBT, KPUBD) et des signatures de certificat (SACT, SACD) d'autorités de certification respectives (ACT, ACD), caractérisé en ce que, après une sollicitation de délégation (E1) du délégué (D) par le titulaire
15 (T), il comprend les étapes suivantes :
- dans le terminal de délégué (TED), un établissement (E2) d'une requête de re-certification (RRC) et une transmission (E3) de la requête de certification (RRC) au terminal de titulaire (TET),
20 - un établissement (E5) d'un deuxième certificat de délégué électronique (C2D) dans le terminal de titulaire (TET) en réponse à la requête de re-certification, et une transmission (E6) du deuxième certificat au terminal de délégué (TED), le deuxième
25 certificat (C2D) incluant des données telles que la clé publique du titulaire (KPUBT), la clé publique de délégué (KPUBD) et un attribut de délégation (ATD), et une signature (ST) des données avec une clé privée (KPRT) du titulaire,
 - 30 - dans le terminal de délégué (TED), une validation (E7) de la signature (ST) dans le deuxième certificat de délégué transmis (C2D) afin que le terminal (TED) utilise le deuxième certificat validé (C2D) pour toute action déléguée par le titulaire (T)
35 au délégué (D).

2 - Procédé conforme à la revendication 1, selon lequel les données dans le deuxième certificat de délégué (C2D) incluent une durée de délégation (DD).

5

3 - Procédé conforme à la revendication 1 ou 2, selon lequel les données dans le deuxième certificat de délégué (C2D) incluent des informations à une révocation du deuxième certificat.

10

4 - Procédé conforme à l'une quelconque des revendications 1 à 3, selon lequel le certificat de titulaire (CT) est inclus dans les données du deuxième certificat de délégué (C2D).

15

5 - Procédé conforme à l'une quelconque des revendications 1 à 4, selon lequel un attribut (ATT) représentant une autorisation du titulaire (T) à déléguer est inclus dans le certificat de titulaire (CT).

20

6 - Procédé conforme à l'une quelconque des revendications 1 à 5, comprenant une détermination (E22) d'une signature (SKD) de la clé publique (KPUBD) du délégué (D) dans le terminal de délégué (TED) en fonction d'une clé privée (KPRD) du délégué, la clé publique de délégué (KPUBD) et la signature (SKD) étant introduites dans la requête de recertification (RRC), et une validation (E44, E45) de la signature (SKD) extraite de la requête de recertification reçue en fonction de la clé publique de délégué (KPUBD) par le terminal de titulaire (TET), avant l'établissement (E5) du deuxième certificat de délégué (C2D).

35

7 - Procédé conforme à l'une quelconque des revendications 1 à 6, comprenant une génération (E23) de deuxièmes clés publique et privée de délégué (KPUB2D, KPR2D) dans le terminal de délégué (TED), la
5 deuxième clé publique (KPUB2D) étant incluse dans la requête de re-certification (RRC), puis introduite dans le deuxième certificat de délégué (C2D) à la place de la clé publique respective de délégué (KPUBD) par le terminal de titulaire (TET).

10

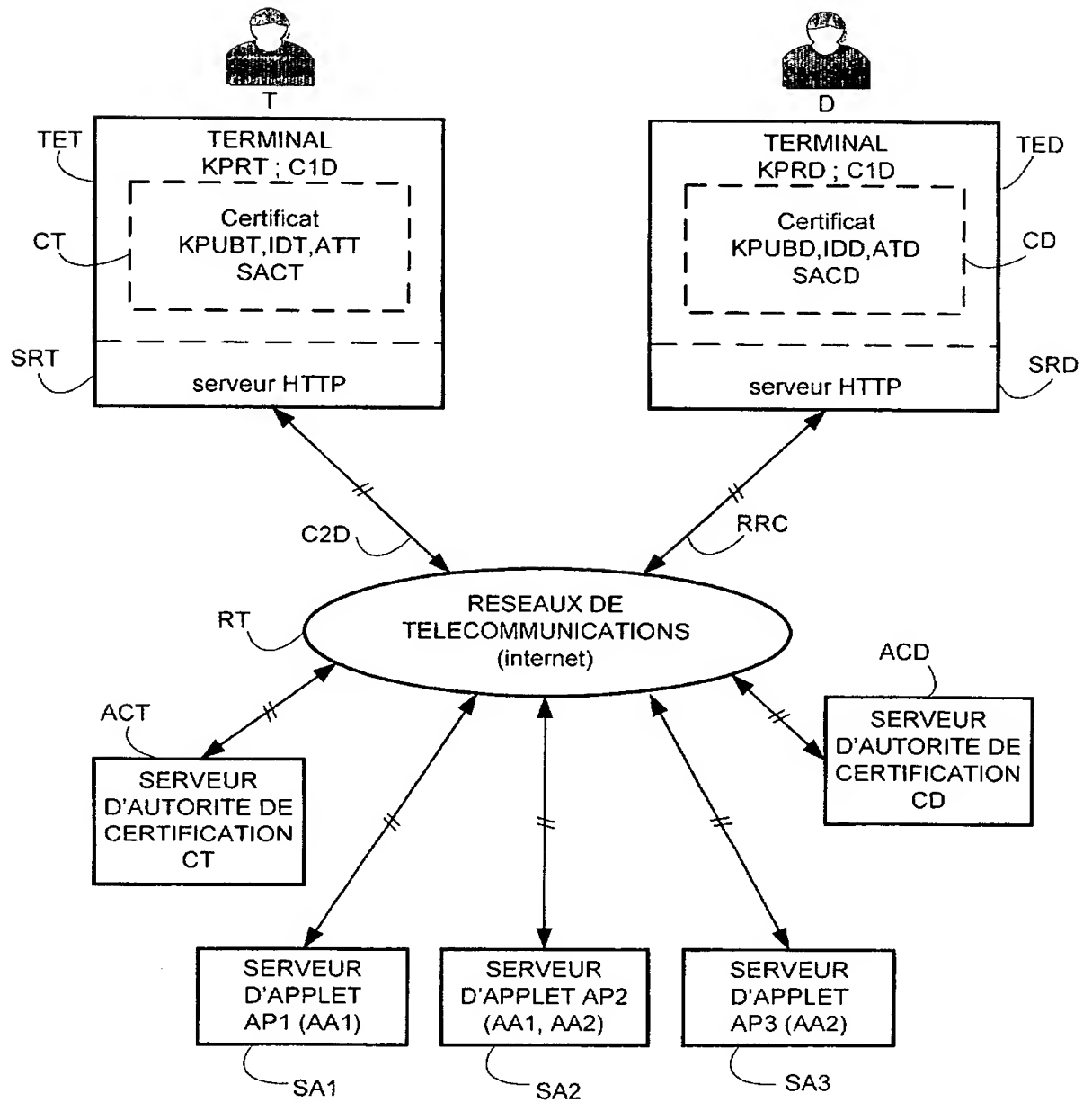
8 - Procédé conforme à l'une quelconque des revendications 1 à 5, comprenant une génération de la clé privée (KPRT) du titulaire (T) dans le terminal de titulaire, à la place de l'établissement (E2) et
15 la transmission (E3) de la requête de recertification, afin d'établir (E5) la signature (ST) des données avec ladite clé privée et de transmettre (E6) ladite clé privée sensiblement en parallèle avec le deuxième certificat de délégué
20 électronique (C2D) au terminal de délégué (TED).

9 - Procédé conforme à l'une quelconque des revendications 1 à 8, selon lequel le deuxième certificat de délégué (C2D) est enregistré dans un
25 support d'enregistrement amovible du terminal de délégué (TED).

30

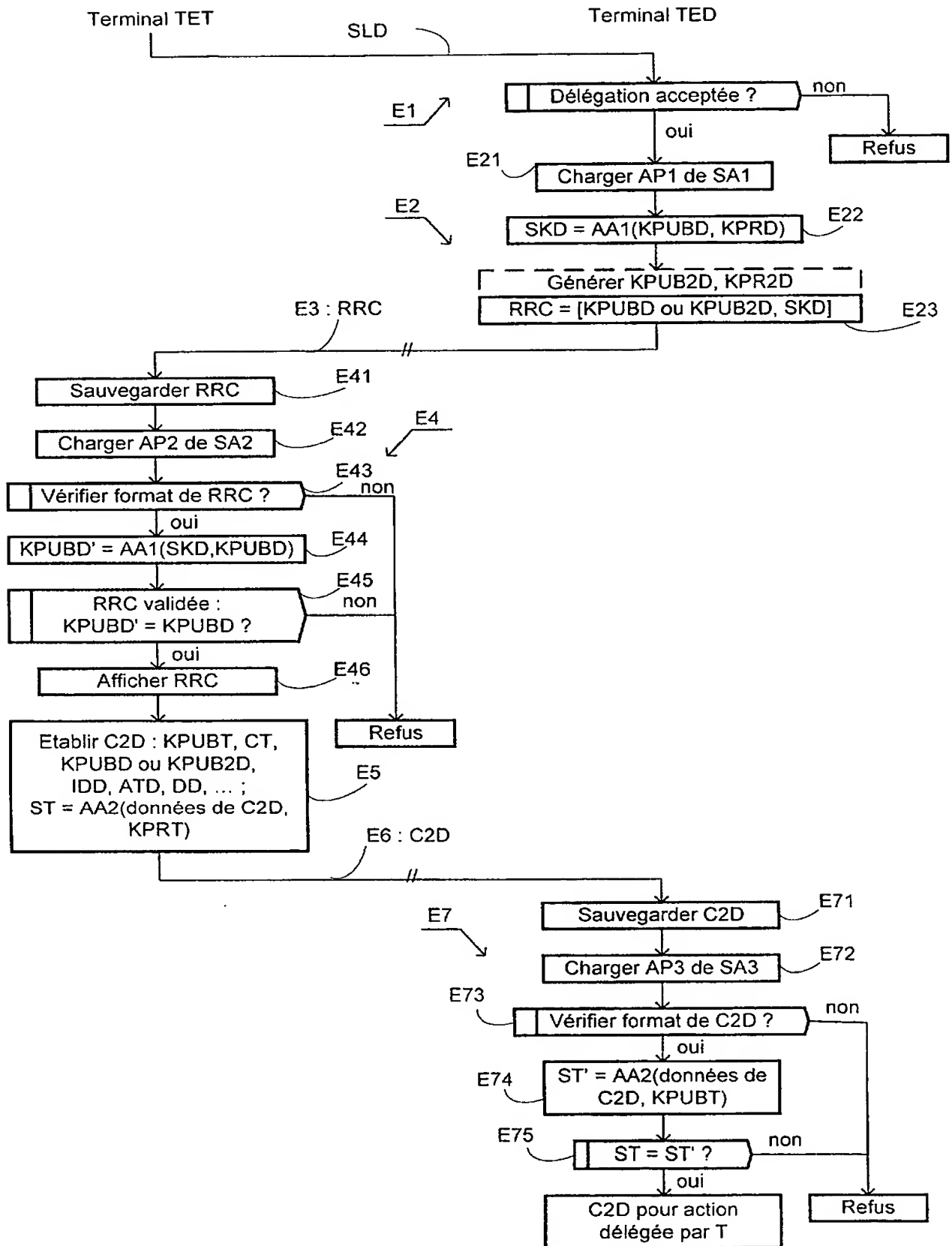
1/2

FIG. 1



2/2

FIG. 2



**BREVET D'INVENTION****CERTIFICAT D'UTILITÉ**

Code de la propriété intellectuelle - Livre VI

N° 11235*03
DÉPARTEMENT DES BREVETS
 26 bis, rue de Saint Pèresbourg
 75800 Paris Cedex 08

Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° 1.../1...

(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)

INV

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 G W / 27C501

Vos références pour ce dossier (facultatif)		SD/CNET04396
N° D'ENREGISTREMENT NATIONAL		0213179
TITRE DE L'INVENTION (200 caractères ou espaces maximum)		
Délégation par certificat électronique		
LE(S) DEMANDEUR(S) :		
FRANCE TELECOM 6, Place d'Alleray 75015 PARIS		
DESIGNE(NT) EN TANT QU'INVENTEUR(S) :		
1	Nom	CAMUS
	Prénoms	Sylvie
Adresse	Rue	2, rue du 11 Novembre Bât. A1
	Code postal et ville	91120 PALAISEAU
Société d'appartenance (facultatif)		
2	Nom	FRISCH
	Prénoms	Laurent
Adresse	Rue	27, avenue d'Italie
	Code postal et ville	75013 PARIS
Société d'appartenance (facultatif)		
3	Nom	MOUTON
	Prénoms	Dimitri
Adresse	Rue	11, rue Antoine Bourdelle
	Code postal et ville	75015 PARIS
Société d'appartenance (facultatif)		
S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.		
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)		
Roland LAPOUX Mandataire CPI/92-1136		 Le 21 Octobre 2002